Picture credit: Getty

RISE OF THE LONE WOLF

Mark Brace *looks at the rise of the solo actor terrorist attack on airports and wonders what can be done to fight back*

A vehicle filled with gas canisters was rammed into the entrance of Glasgow International airport in 2007

Metrojet. 9/11. The transatlantic flight liquid explosives plot. The Underwear Bomber. All well-planned attacks. Some sophisticated, some crude, mostly effective and – in different ways – they changed aviation security. All were perpetrated by large cells and/or had the backing of well-resourced extremist organisations, whether through centralised planning and tasking, innovative bomb-making expertise or extensive support networks. Typically, terrorist attacks targeting aviation require planning, training, support, resources and techniques in different measures in order to defeat the layers of security protecting the industry. Presumably, then, it's beyond the reach of 'lone wolf' attackers?

In recent years there has been a general rise in lone wolf extremists – there is unfortunately a long list of attacks that have taken place in a range of countries, including the UK, France, Germany, Canada, Australia, the USA and Israel, perpetrated by radicalised individuals using a variety of methodologies, such as bladed weapons, improvised explosive devices (IEDs) and vehicle ramming. These have been aimed at the general public, crowded places or individual members of the security forces in areas considered safe – all perceived as soft(er) targets. This is one way that aviation fits into the target set – airports are a classic example of a crowded place, filled with members of the public in an enclosed space. Added to the fact that aviation has always been an attractive, high-impact, headline-grabbing target for terrorists, and it ticks all the boxes. However, security enhancements introduced in recent years mean that airports are not as vulnerable as they once were.

While attacks such as those at Brussels and Istanbul airports in 2016 were carried out by cells supported or facilitated by a major terrorist organisation, the Islamic State of Iraq and the Levant (ISIL), there are examples of attacks by lone wolves (or small groups of two or three individuals). In 2007, two Islamist extremists failed in an attempt to detonate two vehicle-borne IEDs (VBIED) in central London, then made a similar attempt to attack Glasgow International Airport a few days later. They rammed a vehicle filled with petrol containers and gas canisters into an entrance to the airport's terminal building, but only succeeded in setting fire to the vehicle and damaging the entrance. As a direct result of this, physical security was bolstered at airport terminal entrances across the UK, and vehicle access was limited.

But who are these lone wolves? They are typically not formally attached to any extremist organisation and may have self-radicalised in isolation from others of a similar mindset. Some have been pejoratively labelled 'bedroom jihadis' – individuals who live with their parents and access material online, from radicalisation propaganda through to instructional bomb-making videos, or perhaps encourage each other on social media and internet forums. They might be vulnerable or easily led, perhaps psychologically predisposed to pursuing radical ideologies or violent activity, ready to latch onto the cause of the day (there are examples of far-right extremists who have become Islamists). They might also be individuals whose efforts to travel to fight, for example for ISIL in Syria/Iraq, may have been frustrated, so they have done what they consider they next best thing – or only other option – and planned an attack on their home soil.

In addition to foreign fighters returning from conflict zones – such as those who joined ISIL – bringing experience and training to potentially carry out attacks in their home countries, the general migration of terrorist tactics and know-how is a continuing phenomenon. A key concern is the proliferation of these ideas and the associated technology, for example the weaponisation of drones. The availability and sophistication of commercial off-the-shelf drones has improved exponentially in recent years, making the use of a drone in a terrorist attack by a lone actor a feasible option – and one that could be used against aviation targets. There have been plenty of examples in recent years of internet-inspired lone actors planning attacks against other 'soft' targets using such techniques.

By their very nature, lone actors can slip under the radar of investigators. There is a reliance on security and intelligence agencies looking for warning signs and identifying likely candidates. As successes in uncovering plots by larger cells have increased, cases involving lone actors have risen. How do they find lone wolves? It might seem like a near-impossible task before it's too late, like searching for the proverbial needle in a haystack. However, mistakes are made and clues left – for example, attempting to obtain illegal items such as weapons, chemical or other IED components, or perhaps saying too much in a chat room or in the company of others. The latter example might give investigators a crucial lead to infiltrate attack planning. In August 2019, US police arrested a Pakistan-born US national in the late stages of planning a knife attack in New York City in the name of ISIL. The individual allegedly sought to carry out his planned attack at a waterfront promenade area located close to the city's LaGuardia Airport. While the plot may not have been targeting the airport specifically, the marauding nature of the planned attack could have posed a threat to the facility and those using it. However, undercover investigators were reportedly in contact with the suspect and likely exercised some element of control over the plot, enabling timely executive action to be taken. It might be argued that the suspect would not have gone as far as to carry out an attack if he was not encouraged to do so or provided with the means, which may have come from the undercover officers. Entrapment laws covering these scenarios differ across the world.

AVIATION HAS ALWAYS BEEN A HIGH-IMPACT, HEADLINE-GRABBING TARGET FOR TERRORISTS

Airport buildings and facilities could be targeted by lone actors without gaining access to secure areas, for example via the use of emplaced and/or remotely detonated IEDs. They do not even have to be genuine to cause disruption – as well as hoax threat calls, hoax IEDs are part of the lone actor's arsenal. In January 2020, a suspect device was discovered by security forces outside the terminal building at Mangalore International Airport in India. While it was unclear whether it was a fully functioning IED, component parts including explosive material were reportedly present. The suspect – who gave himself up two days later – was known to police, as he had previously made hoax calls to Bangalore's Kempegowda International Airport in 2018 and apparently held a grudge after being rejected for a job at the airport. While it is unclear why he made the jump from hoax calls to IEDs, there was no indication of any terrorist links or accomplices, and media reporting suggested he had used online instructional material to construct his IED.

A much greater challenge for a lone actor is defeating airport security checks in order to get a device or weapon on board a flight. Terrorist groups such as al-Qaeda have attempted numerous attacks over the years using sophisticated concealed IEDs designed to defeat the extensive security measures found in modern airports. This is beyond the capability of the vast majority of lone actors, although al-Qaeda in the Arabian Peninsula (AQAP) provided instructions for what appeared to be a version of its 2009 'underwear bomb' – an IED containing no metal components – in a December 2014 issue of its online magazine *Inspire*,

intended to be used to target commercial airliners. There have been no known attempts to replicate this device, although publications such as *Inspire* and ISIL's *Dabiq* have provided motivation, inspiration and practical advice to lone actors.

A more attainable way of breaching airport security is using hoax devices. In March 2016, a passenger claiming to be wearing an explosive belt hijacked an EgyptAir flight, forcing it to land in Cyprus. He had constructed the hoax device using innocuous items he had in his hand luggage, so there had been no breach of security at the departure airport. The hijack ended peacefully; the perpetrator – an Egyptian national – had demanded to see his estranged wife in Cyprus and had no known terrorist links. In a similarly motivated hijack in Bangladesh in February 2019, a passenger hijacked a Biman Airlines flight from Dhaka's Hazrat Shahjalal International Airport using what was reported to be a replica or toy gun; he also had a fake 'explosive vest'. His demands were to speak to his wife and the Bangladeshi Prime Minister; he died after being shot during a raid on the aircraft on the ground. It is unclear exactly where and how security was breached at Dhaka Airport, enabling the replica firearm to be taken on board.

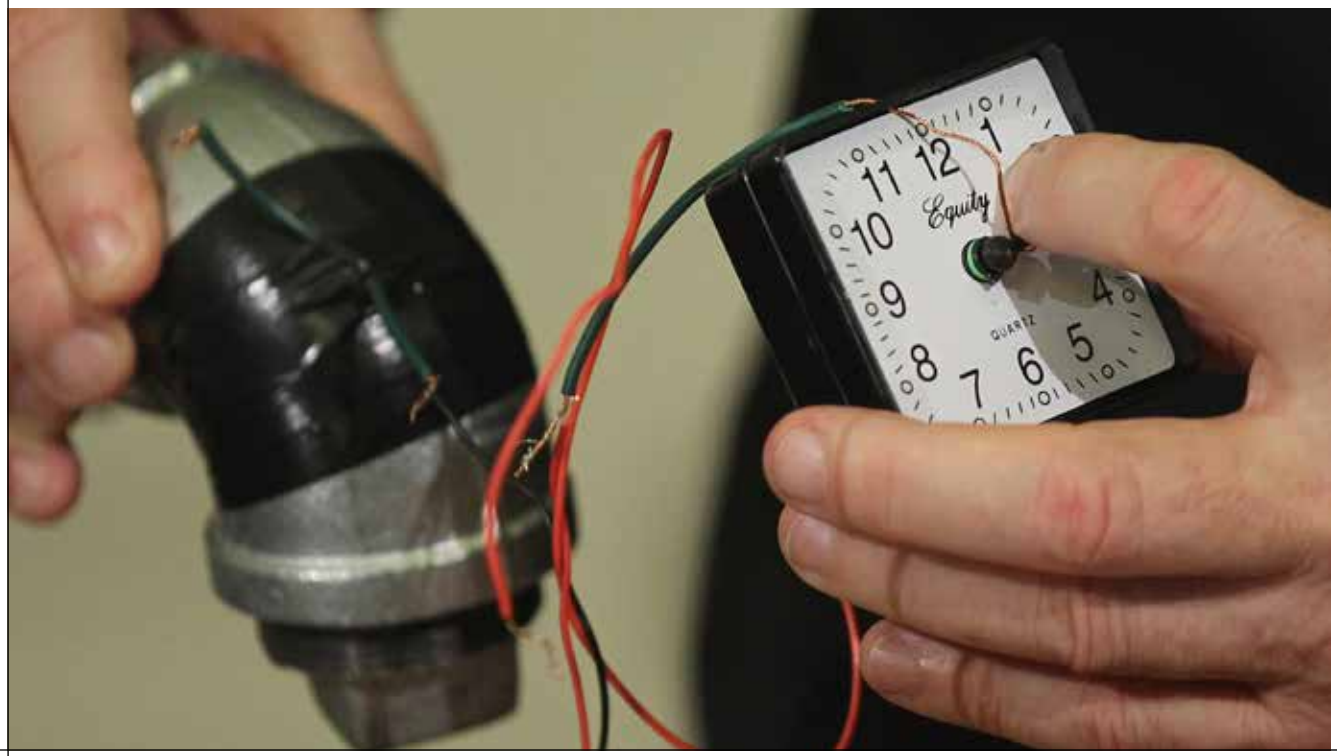
Despite the incidents described above, aviation security still retains a deterrent effect – perceived or otherwise – when it comes to lone wolves. In March 2019, the US authorities arrested an ISIL-supporting individual who had rented a vehicle to carry out a ramming attack at Washington-Dulles International Airport. He reportedly deemed the airport unsuitable for such an attack after attempting to access restricted areas and deciding the crowds were too small. He therefore changed his focus to a popular waterfront destination near Washington DC, where he was arrested. This reflected the capability of the aviation infrastructure within the US to effectively adapt to amorphous terrorism challenges, as it highlighted the deterrent effect that appropriate security measures can have at landside locations outside airport terminal buildings, as well as methods to reduce concentrations of people at these locations.

Of course, a lone wolf could be an airport or airline insider, potentially rendering some of the most sophisticated security mechanisms useless. This could take the form of a pilot or other employee with appropriate access commandeering an aircraft without permission, as happened in August 2018 at Seattle-Tacoma International Airport when an airline ground service agent stole a Horizon Air Dash 8 Q400 airliner. He managed to take off and carry out aerobatic manoeuvres before deliberately crashing the aircraft in an uninhabited area. It was later confirmed the incident was not terrorism-related and that the individual responsible was suffering from mental health issues. In March 2020, a former American Airlines mechanic was sentenced to three years' imprisonment after pleading guilty to sabotaging an aircraft at Miami International Airport in July 2019. He glued a piece of foam inside a navigation system on an aircraft, resulting in an error message being generated and the aircraft aborting its take-off; the mechanic claimed he wanted to create more overtime work, as well as being upset over stalled union contact negotiations. No evidence was found of any terrorist links after allegations of such connections had arisen in September 2019.

Aviation is a challenging target for would-be lone wolf attackers. But this won't stop them trying, no matter how misguided. By their nature, they are likely to attempt attacks regardless of the odds of them succeeding. Even failed attempts are likely to result in significant disruption to aviation operations more widely, as short-term security enhancements are implemented while investigators attempt to establish what happened and how to stop it occurring again. This in turn could lead to new longer-term security procedures, causing financial impact to the industry and inconveniencing the travelling public. The key challenge is identifying perpetrators before it's too late, so having an effective working relationship with security forces and revising internal mechanisms for suspicious activity, safety and security reporting is as crucial as having robust security checks, procedures and deterrents in place ●

Mark Brace – Senior Aviation Security Analyst at Osprey Flight Solutions – has many years' experience as a senior threat analyst for the UK Government, with specific expertise in threats to aviation.

Remotely detonated IEDs do not even have to be genuine to cause disruption to an airport



Picture credit: Getty